COSC 683 Security and Internet Algorithms

Notes on Finite Fields

Lecturer: Marius Zimand *Scribe: Marius Zimand*

This is a brief summary on finite fields. The document is a based on some notes written by Clifford Bergman.

INFORMAL DEFINITION: A *field* is a set of "numbers" that can be added, subtracted, multiplied, and divided.

Examples:

- $\mathbb{Q}$ = rational numbers
- $\mathbb{R}$ = real numbers
- $\mathbb{C}$ = compleXnumbers
- $\mathbb{Z}_p$ when p is prime (the set of integers with addition and multiplication modulo 5)

Many applications require finite fields, because computers do not handle well infinite objects since they can only store an approximation of an infinite object. Only $\mathbb{Z}_p$ in the above list is a finite field.

Definition 1. *A field is a structure $(F, +, \cdot, 0, 1)$ in which F is a nonempty set, $0, 1 \in F$ are some some special elements and such that for every $X, y, z \in F$,*

1. $(x + y) + z = x + (y + z)$
2. $x + y = y + x$
3. $x + 0 = x$
4. *there is $-x$ such that* $x + (-x) = 0$
5. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
6. $x \cdot y = y \cdot x$
7. $x \cdot 1 = x$
8. *if $x \neq 0$, there is x^{-1} such that* $x \cdot x^{-1} = 1$
9. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$

In what follows, F denotes a finite field.

POLYNOMIALS

Polynomials are used to extend a field F to a larger field F', so that $F \subset F'$.

Let F be a field. A polynomial over F looks as follows:

$$g(X) = a_k X^k + a_{k-1} X^{k-1} + \ldots + a_1 X + a_0,$$

where $a_o, a_1, \ldots, a_k \in F$.

If $a_k \neq 0$, then g has degree k.

If $a_k = 1$, then g is *monic*.

$F[X]$ denotes the set of all polynomials over F.

Polynomials can be added, subtracted, and multiplied in the usual way.

Ex: Take $F = \mathbb{Z}_5$:

$$(X^4 + 3X - 4) + (X^4 - 4X - 2) = (2X^4 - X - 1)$$

$$(X^4 + 3X - 4)(X^3) = (X^7 + 3X^4 - 4X^3)$$

Note that the exponents are not reduced modulo 5.

Let's look at division of polynomials. We try to divide $3X^3 + 2X^2 + 1$ by $X^2 + 2X - 1$.

$$3X^3 + 2X^2 + 1 = (3X + 1)(X^2 + 2X - 1) + (X + 2).$$

In general:

If $f(X), g(X) \in F[X]$ and $g(X) \neq 0$

then there are unique polynomials $q(X), r(X) \in F[X]$ such that

$f(X) = q(X)g(X) + r(X)$ and $deg(r) < deg(q)$.

Let $f(X), g(X) \in F(X)$. We say that $g(X)$ divides $f(X)$ (notation $g(X)|f(X)$) if there is $q(X)$ such that $f(X) = q(X)g(X)$.

Theorem 2. *Let $f(X) \in F[X]$ and $a \in F$. Then $(X - a)|f(X) \Leftrightarrow f(a) = 0$.*

Definition 3. *A polynomial $f(X)$ is* irreducible *if its only divisors are of the form a and $af(X)$ for some $a \in F$. (In other words, $f(X)$ cannot be written as the product of two polynomials of degree ≥ 1.)*

Irreducible polynomials are similar to prime numbers.

Let $f(X), g(X), h(X) \in F[X]$. We say

$$f(X) = g(X) (\text{mod } h(X)) \Leftrightarrow h(X) | (f(X) - g(X)).$$

It is easy to see that $f(X) = g(X) \pmod{h(X)}$ iff f and g leave the same remainder when divided by h.

Example (over $\mathbb{Z}_5$)

$$2X^2 + 3X = X^2 + 3X + 4 \pmod{X + 2}$$

$F[X]/(h(X))$ = the set of remainder polynomials upon division by h (this is similar to Z_n).

If $deg(h(X)) = k$, then $F[X]/h(X)$ consists of all polynomials of degree less than k.

Thus, $|F[X]/h(X)| = |F|^k$, because there are $|F|^k$ many polynomials of degree $< k$ (make sure you understand this).

Theorem 4 (FIELD EXTENSION THEOREM)**.** *$F[X]/h(X)$ with addition and multiplication modulo $h(X)$ is a field if and only if $h(X)$ is irreducible.*

The FIELD EXTENSION THEOREM tells us how to extend a field F: take an irreducible polynomial h and then $F' = F[X]/h(X)$ is a larger field that contains F as a subfield.

In particular: Let p be a prime number and let $h(X)$ be irreducible of degree k over Z_p. It can be whown that there exists such a polynomial for every natural number $k \geq 2$. Then $Z_p[X]/h(X)$ is a field of order p^k.

Example: We take $F = Z_3[X]/(X^2 + 1)$. The polynomial $X^2 + 1$ is irreducible over Z_3, and thus F is a field. F consists of $\{aX + b \mid a, b \in Z_3\}$ (there are 9 elements in F) and addition and multiplication is done modulo $X^2 + 1$. For example

$$(2X + 1)(X + 1) = (2X^2 + 3X + 1) = 2 (\text{mod } X^2 + 1).$$

The last equality holds because $X^2 = -1$ in F and thus $2X^2 + 3X + 1 = 2 \cdot (-1) + 0 + 1 = -1 = 2$ (recall that the arithmetic of coefficients is in Z_3).

Let $F_1 = Z_3[X]/(X^2 + X + 2)$ and $F_2 = Z_3[X]/(X^2 + 1)$. Do the addition table and the multiplication table of F_1 and F_2. What do we observe? We have an isomorphism $aX + b \mapsto aX + b + 2a$ from F_1 into F_2. (An isomorphism is an application $h : F_1 \longmapsto F_2$ that is 1-to-1 and that "'preserves"' the operations, i.e., for all $x, y \in F_1$, $h(x + y) = h(x) + h(y), h(x \cdot y) = h(x) \cdot h(y)$, $h(0) = 0$ and $h(1) = 1$.)

Theorem 5. *Any two finite fields of the same cardinality are isomorphic. (I.e., essentially they are the same).*

The fundamental theorem about finite fields:

Theorem 6 (FUNDAMENTAL THEOREM OF FINITE FIELDS)**.** *For every prime number p and for every positive integer k there is one and only one field with exactly p^k elements. If n is a number which is not the power of a prime number, then there is no field with n elements.*

Example: There is a field (and only one) with 125 elements, because $125 = 5^3$. There is no field with 30 elements because 30 is not the power of aprime number.

The unique field with p^k element is usually denoted GF(p^k) (GF stands for Galois field).

For example, say we need a field with 8 elements. First of all, there is such a field because 8 is a power of 2. How do we get it? Note that $8 = 2^3$. Thus we need an irreducible polynomial over Z_2 of degree 3. $h(X) = X^3 + X + 1$ is such a polynomial. So we take $F = Z_2[X]/(X^3 + X + 1)$.

TESTING IRREDUCIBILITY

Let p be a prime number and $f(X) \in Z_p[X]$ has degree n.

1. If $deg(f(X)) \leq 3$ then $f(X)$ is irreducible if and only iff no element in Z_p is a root of f.
2. f is irreducible over Z_p if and only for every $k < n$, $gcd(f(X), X^{p^k} - X) = 1$. (The gcd can be calculated fast with the Euclidean algorithm).

Let F be a finite field. $F^* = F - \{0\}$.

F^* with the multiplication operation inherited from F is a group (i.e., multiplication is commutative, associative, each element has an inverse).

Let $a \in F$. The *cyclic subgroup* generated by a is

$$\langle a \rangle = \{a^k \mid k = 0, 1, 2, \ldots\}$$

Example. Let $F = GF(9) = Z_3[X]/(X^2 + X + 2), \alpha = X + 1, \beta = 2X + 1$. Then

$$\langle \alpha \rangle = \{1, X + 1, X + 2, 2X, 2, 2X + 2, 2X + 1, X\} = F^*.$$

$$\langle \beta \rangle = \{1, 2X + 1, 2, X + 2\}.$$

Definition 7. *The order of an element $\alpha \in F$ is the smallest k such that $\alpha^k = 1$.*

Theorem 8. *Let F be a field with p^n elements. Then the order of any element of F^* is a divisor of $p^n - 1$. Also for every $\alpha \in F^*$, $\alpha^{p^n - 1} = 1$.*

This implies the roots of the polynomial $X^{p^n} - X$ are exactly the p^n elements of the field F.

Definition 9. *$\alpha \in F$ is called primitive (or a generator) if $\langle \alpha \rangle = F^*$. This is the same as saying that α has order $|F^*|$, which recall is $p^n - 1$*

Theorem 10. *Every finite field has a primitive element (a generator).*

Theorem 11. *$GF(p^m)$ is a subfield of $GF(p^n)$ if and only if m divides n.*

Minimal polynomials

Definition 12. *Let F be a field of order p^n, let $\beta \in F$. The minimal polynomial of β is the polynomial g, which is the monic polynomial of smallest degree in $Z_p[X]$ such that $g(\beta) = 0$.*

g the minimal polynomial of β has the following properties:

- for any polynomial $h(X)$, $h(\beta) = 0 \Leftrightarrow g(X)|h(X)$.
- $g(X)$ is irreducible.
- $deg(g(X)) \leq n$.

If α is a primitive element of $GF(p^n)$, then the minimal polynomial for α is called a *primitive polynomial* of $GF(p^n)$.

Theorem 13. *Let $f \in \mathbb{Z}_p[X]$ be a polynomial of degree n. Then f is a primitive polynomial of $GF(p^n)$ if and only if f is irreducible and the smallest m such that $f(X)$ divides $X^m - 1$ is $m = p^n - 1$.*

Some examples of finite fields, representations, primitive element, etc.

Example 14. The multiplication tables of the field $GF(4)$ obtained as $GF(2)[X]/X^2 + X + 1$.

addition table

+	0	1	X	X+1
0	0	1	X	X+1
1	1	0	X+1	X
X	X	X+1	0	1
X+1	X+1	X	1	0

multiplication table

×	0	1	X	X+1
0	0	0	0	0
1	0	1	X	X+1
X	0	X	X+1	1
X+1	0	X+1	1	X

For instance: $X(X+1) = X^2 + X = X + 1 + X = 1$

$(X+1)(X+1) = X^2 + 2X + 1 = X^2 + 1 = X + 1 + 1 = X$.

Example 15. Representations of the field $GF(8)$ obtained as $GF(2)[X]/(1 + X + X^3)$:

GF(8) admits the following three representations, given in the columns of the table below. α is a generator (meaning that $\alpha^0, \alpha^1, \alpha 2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ are all the non-zero elements of GF(8). In this example, we have taken $\alpha = X$, and the last column shows that indeed α is a generator of GF(8). To give just one example, $\alpha^6 = X^6 = (X^3)^2 = (1 + X)^2 = 1 + X^2$.

polynomial	binary	α powers
0	0,0,0	-
1	0,0,1	α^0
X	0,1,0	α^1
$1 + X$	0,1,1	α^3
X^2	1,0,0	α^2
$1 + X^2$	1,0,1	α^6
$X + X^2$	1,1, 0	α^4
$1 + X + X^2$	1,1,1	α^5